SCTE · ISBE

STANDARDS

Data Standards Subcommittee

SCTE STANDARD

SCTE 266 2021

IoT Recommended Premises Network Infrastructure Practices for Cable Operators

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) / International Society of Broadband Experts (ISBE) Standards and Operational Practices (hereafter called "documents") are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interoperability, interchangeability, best practices, and the long term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE•ISBE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE•ISBE members.

SCTE•ISBE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

NOTE: The user's attention is called to the possibility that compliance with this document may require the use of an invention covered by patent rights. By publication of this document, no position is taken with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from the standards developer. SCTE•ISBE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE•ISBE web site at https://scte.org.

140 Philips Road
Exton, PA 19341

Document Types and Tags

Document Type: Operational Practice

Document Tags:

☐ Test or Measurement	☐ Checklist	☐ Facility
☐ Architecture or Framework	☐ Metric	☐ Access Network
☒ Procedure, Process or Method	☐ Cloud	☒ Customer Premises

Table of Contents

Title **Page Number**

List of Figures

List of Tables

1. Introduction

1.1. Executive Summary

This recommended practices document contains the considerations and recommendations for operators with regards to the premises network infrastructure for residential as well as small to medium businesses.

These are recommendations and should not be considered requirements. The final design is the responsibility of the implementer.

1.2. Scope

The following areas are covered within this document:

1. Premises Construction Considerations
2. Wired Protocol Considerations
3. Wireless Protocol Considerations
4. Power Considerations
5. Installer Best Practices
6. Customer Support Best Practices

1.3. Benefits

This document will be used to provide the following benefits:

- Educate the service providers on the considerations for IoT in various premises
- Develop methods and procedures for installation
- Develop customer support

1.4. Intended Audience

The intended audience are service provider engineering, operations, field service, and care teams.

1.5. Areas for Further Investigation or to be Added in Future Versions

None at this time.

2. Normative References

The following documents contain provisions, which, through reference in this text, constitute provisions of this document. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision; and while parties to any agreement based on this document are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version.

2.1. SCTE References

No normative references are applicable.

2.2. Standards from Other Organizations

No normative references are applicable.

2.3. Published Materials

No normative references are applicable.

3. Informative References

The following documents might provide valuable information to the reader but are not required when complying with this document.

3.1. SCTE References

[Battery] NCTA Methods to Maximize IoT Battery Life, https://www.nctatechnicalpapers.com/Paper/2019/2019-methods-to-maximize-iot-battery-life

3.2. Standards from Other Organizations

[Bicsi] Bicsi Information Technology Installation Methods Manual (7th edition), https://www.bicsi.org/education-certification/education-@-bicsi-learning-academy/technical-publications/information-technology-systems-installation-methods

3.3. Published Materials

No informative references are applicable.

4. Compliance Notation

shall	This word or the adjective "***required***" means that the item is an absolute requirement of this document.
shall not	This phrase means that the item is an absolute prohibition of this document.
forbidden	This word means the value specified shall never be used.
should	This word or the adjective "*recommended*" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighted before choosing a different course.
should not	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
may	This word or the adjective "*optional*" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.
deprecated	Use is permissible for legacy purposes only. Deprecated features may be removed from future versions of this document. Implementations should avoid use of deprecated features.

5. Abbreviations and Definitions

5.1. Abbreviations

AAA	authentication, authorization, and administration
AC	alternating current
CA	certificate authority
COAM	customer owned and managed
CPE	customer premises equipment
CPU	central processing unit
CRC	cyclic redundancy code
DC	direct current
DHCP	dynamic host configuration protocol
DNS	domain name system
DNS RPZ	domain name service response policy zones
DNSSEC	domain name system security extensions
DOCSIS	Data Over Cable Service Interface Specification
DRAM	dynamic random access memory
DSM-CC	digital storage media – command & control
EEROM	electrically erasable read only memory
FIPS	federal information processing standard
FLUTE	file delivery over unidirectional transport
FQDN	fully qualified domain name
FTP	file transfer protocol
HDD	hard disk drive
HTTP	hyper text transfer protocol

HTTPS	hyper text transfer protocol secure
IoT	Internet of things
IP	Internet protocol
IV	initialization vector
JTAG	joint test action group (IEEE Standard 1149.1-1990)
LED	light emitting diode
MAC	media access control
MDU	multiple dwelling unit
OCF	open connectivity foundation
OS	operating system
PCB	printed circuit board
POC	point of contact
QA	quality assurance
RDK	reference design kit
ROM	read only memory
SCTE	Society of Cable Telecommunications Engineers
SD	secure digital
SFH	single family home (aka SFU)
SFU	single family unit (aka SFH)
SMB	small to medium business
SNMP	simple network management protocol
SoC	system on chip
SRAM	static random access memory
SSH	secure shell
SSM	source-specific multicast
TFTP	trivial file transfer protocol
TR	technical report
UI	user interface
URL	uniform resource locator
USB	universal serial bus

5.2. Definitions

asymmetric encryption	Also called public-private key cryptography. Utilizes one key to encrypt and a different key to decrypt.
attack	Any cybersecurity method which is actively being used to gain unauthorized access to or control of an IoT device or the data associated with an IoT device.
attenuation	Loss of intensity for an electrical signal passing through a material.
authentication	Methods that are used to ensure that IoT data comes from trusted sources.
encryption	Encoding a message in a way that only authorized users can access it, usually requiring a key. Encryption is a higher order of obfuscation.
galvanic action	An electrochemical process in which one metal corrodes preferentially when in electrical contact with another.
mesh network	A local network topology in which all devices connect directly, dynamically, and non-hierarchically to as many other devices as possible and cooperate with one another to efficiently route data from/to clients. These networks dynamically self-organize and self-configure.
obfuscation	Method used to mask data except for authorized users. It can be simple, e.g. reversing the order of bits, exclusive or with a known value, etc., or complicated such as with encryption.
persistent memory	Any memory device which retains the data when there is no power.
symmetric encryption	The same key can be used for the encryption and decryption of data.
unlicensed spectrum	RF spectrum that does not require a license to utilize. Examples are Wi-Fi, ZigBee, Z-Wave, and Bluetooth.
vulnerability	Any cybersecurity gap or flaw which could be used to gain unauthorized access to data or control of an IoT device or the data associated with an IoT device.

6. Premises Construction Considerations

The type of construction that is utilized within premises can make a drastic impact on the installation of an IoT system. In some types of construction, wireless signals can be impeded while others can make wiring very difficult. This section will address these issues and offer suggestions on how to mitigate them.

6.1. Construction Materials

In the United States, wood is the most common structural material for homes and small businesses but in some cases masonry and/or steel *may* be the material of choice. Siding can be brick, masonry, wood, aluminum, stucco, or other material. Interior wall and floor structures are typically wood, masonry, or steel while the wall itself is usually either drywall or plaster. In all these cases, there are exceptions.

Other countries will often have different materials and require their own specific planning needs.

Plaster walls offer significant challenges for both wired and wireless installations. For wired installations, care must be taken when drilling into plaster walls (as some can be fairly old), in fact, it is preferable not

to drill into them. The lath (as shown in Figure 1) behind the plaster can also offer challenges. For wireless installations, the lath many times incorporates metal, such as chicken wire, which greatly attenuates RF signals.

Figure 1 - Plaster Lath

6.2. Historical Buildings

In the United States, buildings can be designated as historic by the local, state, or federal government. The regulations for each is different so it is strongly recommended that the service provider become familiar with the ones for their state and local governments as well as the national requirements. This can affect how an IoT system is installed within such a building. Further discussion is outside the scope of this document.

Many other countries have similar regulations. Again, it is important for the service provider to be aware of these regulations.

6.3. Construction Material RF Attenuation

All materials have some RF attenuation, and it varies depending on the frequency. The following table is an example of common construction materials and the associated attenuation at 2.4 GHz, which is the frequency band utilized for ZigBee and 2.4 GHz Wi-Fi.

Table 1 - Attenuations at 2.4 GHz

Building Material	Attenuation For 2.4 GHz (in dB)
Solid Wood Door 1.75"	6
Hollow Wood Door 1.75”	4
Interior Office Door w/Window 1.75”/0.5”	4
Steel Fire/Exit Door 1.75"	13
Steel Fire/Exit Door 2.5"	19
Steel Rollup Door 1.5"	11
Brick 3.5"	6
Concrete Wall 18"	18
Cubical Wall (Fabric) 2.25”	18
Exterior Concrete Wall 27"	53
Glass Divider 0.5"	12
Interior Hollow Wall 4"	5
Interior Hollow Wall 6"	9
Interior Solid Wall 5"	14
Marble 2"	6
Bullet-Proof Glass 1"	10
Exterior Double Pane Coated	13
Glass 1"	13
Exterior Single Pane Window 0.5”	7
Interior Office Window 1"	3
Safety Glass-Wire 0.25"	3
Safety Glass-Wire 1.0"	13

Typically, the attenuation for lower frequencies is directly tied to the frequency (e.g. 6 dB for a 2.4 GHz material would be 3 dB for a 1.2 GHz), however, there is usually a frequency for a given material which will have higher attenuation.

6.4. Wireless vs. Wired

As a rule, wired connections are very controllable, much more so than wireless, except when it comes to lightning. Any device using a wired connection needs to ensure that noise and surges that come from lightning do not damage the device or cause software problems. This is especially true for ensuring that important persistent memory values cannot be corrupted by a software glitch. In areas which are prone to lightning, external surge protection *should* be considered to minimize the damage to devices. Develop some best practices for minimizing lightning effects. The Bisci Information Technology Systems Installation Methods Manual (7th edition) offers some good practices.

One problem with wired connections is the cost of running the wired connection. If a wired connection is needed and required to penetrate through the wall, then the material that the premises is constructed of can offer challenges and the installers need training in how to handle the different building materials.

6.5. General IoT Architecture

IoT devices can perform some amazing functions, however, they do need to connect to the Internet (that's the "I" in IoT). Most IoT devices are wireless and will need to communicate to a hub device; examples would be a ZigBee hub, a Wi-Fi access point, or a proprietary hub. These in turn need to be powered and connected to the Internet, which for a cable service provider implies a DOCSIS or fiber connection with a gateway in between. All of these can be separate devices or embedded in a single device (e.g. a DOCSIS gateway with ZigBee would be one example). If separate devices are utilized, then usually Ethernet or MoCA is used to connect them.

Some IoT devices connect to existing home wiring, such as a thermostat or doorbell camera. Occasionally, some will require a new wired connection such as supplying power for a wireless camera.

6.6. Single Family Unit (SFU)

SFUs can be constructed of many different materials. As mentioned in section 6.1, the most common primary structural material for residential homes in the United States is wood although concrete and steel studs are not uncommon. Masonry is the exception in the United States but can be the rule in other countries. Even in a wood house, there can be areas which utilize concrete, such as in the basement.

The interior walls and ceilings for modern houses are usually drywall over wood studs. Older homes often utilized plaster walls, which offers a lot of challenges (see section 6.1).

Exterior wall structures for modern houses are usually wood studs with an exterior siding, however, concrete or steel studs are not uncommon. Exterior wall siding can be aluminum, wood, brick, concrete, stucco, or some other material. These offer their own challenges for both wired and wireless connections.

It is important for the service provider to be familiar with the types of homes within their service area to ensure that the installers are trained in proper installation for both wired and wireless devices.

6.7. Multiple Dwelling Unit (MDU)

The structure of MDUs can utilize different construction materials so the focus for this document will be on IoT delivery within a single residential unit. Since the interior walls are generally not owned by the tenant, wired connections *should* be avoided. Wireless devices can follow the same paradigm as in a SFU except that congestion will be more of an issue. For this reason, testing for congestion and selecting the protocol's channel frequency becomes more important. Remote radio management (RRM) is the preferred technique for selecting the optimum channel. However, with care, manual techniques can work just as well.

6.8. Small to Medium Business (SMB)

Like an MDU, SMBs can utilize a wide variety of different construction materials. Great care is required in the installation process and installers need to be well trained to cover this wider variance in construction.

6.9. Enterprise Business

Enterprise businesses tend to each be different and unique, and as such, will not be covered in this document.

7. Wiring Considerations

For this document, wires consist of any hard connection to an IoT device, bridge, hub, or gateway. Examples are power wires, coaxial cable, and Ethernet cable.

7.1. Physical Signal Wiring

Service providers *should* already have best practice guidelines for signal wiring, common examples of which are Ethernet (category 5/6) and coaxial cable. IoT devices with physical wiring *should* follow these guidelines.

Note that when false ceilings are present, the wires *should* not lay on the ceiling tile and *should* be plenum rated.

Additionally, for long run signal wires, shielded cables will offer better performance.

7.2. Physical Power Wiring

Service providers *should* already have best practice guidelines for power wiring, common examples are traditional in-home voltages (e.g. 120 VAC) and low voltage (e.g. 12 VDC). In all cases, local, state, and national codes are to be followed. It is expected that the service provider is already aware of these and has their own practices developed.

Note that when false ceilings are present, the wires *should not* lay on the ceiling tile and *should* be plenum rated.

7.3. Physical Signal and Power Wiring

Power over Ethernet (POE) can be used to carry power to devices. Other protocols can also be used for carrying power but they're not as prevalent. POE needs to be treated as power wiring first over signal wiring and needs to follow the same service provider guidelines as well as local, state, and national codes.

8. Wireless Considerations

For this operational practice, the scope of wireless includes all methods of communicating wirelessly. Popular examples are Bluetooth, ZigBee, Z-Wave, Wi-Fi, and cellular technologies (LTE, 4G, 5G, etc.). Other technologies or modifications to these technologies can also be utilized as well.

8.1. Physical Medium

As a rule, the attenuation of RF signals will follow the inverse square law through air in that the attenuation will decrease by roughly 6 dB every time the distance doubles. The frequency will also affect the attenuation. A signal at 2.4 GHz will attenuate by 40 dB in the first meter, and a signal at 5 GHz will attenuate by 47 dB in the first meter. Therefore, at 4 meters the signal level will attenuate approximately 52 dB for a 2.4 GHz signal, and approximately 59 dB for a 5 GHz signal. By referencing the attenuation of common solid objects (see Table 1), a rough calculation can be given for most instances.

Be aware that there are some physical barriers which offer very high attenuation (see Table 1). These include mirrors, plaster walls, metal walls, stucco siding, energy efficient windows, appliances (e.g. refrigerators), metal screens, and other items commonly found in residential and small businesses. Essentially, anything with metal or a metal covering. These can also form “shadows” where there is no coverage and moving a device just a few feet can make a lot of difference on the RF signal.

There is also planarity to consider. When RF waves are emitted from an antenna, they are emitted in patterns associated with the antenna’s physical geometry. A linear antenna will create waves along the polarity associated with the antenna’s polarity. Generally, reflections will create signals in different polarities, but this cannot always be guaranteed, especially for a given location. The result of this is that just moving the device to a different angle can make a big difference. For this reason, if there is a common device that is used, such as a door sensor, it can reduce issues during installation if the controller device’s access point and the door sensor antenna are in the same plane. The effect of this is to reduce opex during installation. There are several methods to offset this by having multiple antenna’s in the access point which are pointed in different angles (planes). However, this reduces the overall signal strength which can lead to other issues. So care must be taken to balance performance will overall costs.

8.2. Congestion

One of the problems with using ISM bands (e.g. Wi-Fi, Bluetooth, ZigBee) is that the different protocols can interfere with each other. While these protocols do include methods to handle interference, one of the consequences is that the protocols utilized will cause retransmissions if the signal is not received and acknowledged. Retransmissions usually aren’t an issue with AC powered devices, but for battery operated devices, this can have an impact to battery life. If battery replacement is a service offered by the service provider, then this service can drive up the overall expense of service, which one won’t see until after a year or so.

Historically, Wi-Fi access points (AP) are not aware of the Bluetooth and ZigBee signals and will select the one with the least amount of Wi-Fi traffic. If the Bluetooth or ZigBee controllers see this, then they will select a different channel. However, in many cases such as a power outage, the Wi-Fi AP takes longer to boot, so the Bluetooth or ZigBee controller will select a channel, then the Wi-Fi AP will select a channel which causes congestion (and lower battery life). Managing the channel spectrum between the different protocols can go a long way to increasing battery life and saves operational costs later.

As an example, if a ZigBee controller boots up and selects ZigBee channel 18, then if the Wi-Fi AP boots and selects Wi-Fi channel 6, you will have interference. It would be ideal if the Wi-Fi AP selects Wi-Fi channel 1 and the ZigBee controller picks ZigBee channel 28. Cross device interference would be prevented.

8.3. Interference

Interference within the ISM bands can come between known protocols (Wi-Fi, Bluetooth, and Zigbee being the predominate ones in the 2.4 GHz band) and other interference can also occur. The most common interference generator is the microwave oven. When new, these generally do not generate appreciable interference but after much use, the seals can become open enough to generate significant interference. Empirical tests of two units in a local workplace break room showed one to have very little interference while the other had significant interference. Again, this can lead to devices not being able to communicate at all as well as frequent retransmissions leading to rapid depletion of battery life.

Other interference sources exist, such as radar. It is important to be aware of these but also be aware that there might not be anything a technician is able to do to resolve radar interference. Therefore, the service provider *should* have a plan on how to handle this with the customer.

Additionally, sometimes the IoT devices could be a source of interference. In the US, FCC Part 15 is the basis of device certification guidelines for interference. When deploying IoT devices, certification to FCC Part 15 *should* be required. If operating outside of the US, it is important to refer to the authority setting local use device certification guidelines. Also, have a good relationship with the vendor to address any interference that could be sourced by the IoT devices.

9. Power Considerations

All devices require power to operate. There are generally four methods utilized to power to IoT devices and supporting equipment:

- AC Power
- Power over Ethernet (PoE)
- Batteries
- Power over coax

9.1. AC Power

AC power, also called line power, is generally used by equipment which is not mobile and has access to an outlet. An IoT device or support equipment utilizes DC power which requires converting the AC power to DC via a power supply. There are generally two types, internal to the IoT device or support equipment (AC connected), or external to the IoT device or support equipment (e.g. wall wart or brick type power supply, DC connected).

With the AC connected devices, proper care must be taken in the position of the power cable to follow known best practices and electrical codes to ensure that the cable is not damaged and cannot be damaged by common use. Additionally, the correct gauge *should* be utilized, and any extension cords used support sufficient current as to not cause any issues.

With DC connected devices, the lower voltage allows for more lax cable wiring, but care *should* still be taken to prevent any damage to the cable, such as fraying or running over sharp edges. Additionally, the power supply itself (the wart or brick) needs to be placed not only in a location where it would not be damaged but that the heat of the unit can be dispersed. Note that the length of the DC cable is generally limited to prevent too much voltage loss, in addition voltage regulation becomes more difficult when a longer cable is utilized unless the power supply is engineered appropriately.

One of the issues that arises is insufficient power outlets. Be sure to have a good extension plan to allow for this.

Voltage fluctuations, voltage surges, brownout, missed cycles, etc. need to be considered, generally by the design of the device itself. It is strongly recommended that extensive testing be completed to know the devices capabilities, and to spot any weak areas prior to procuring and standardizing on said device. If the device has significant cost and/or needs to be reliable, a good surge protector is recommended. If a device needs to be operational even if power is lost, then either it *should* either have built in battery backup or utilize an UPS (uninterruptable power supply). Note that most UPS units also provide surge protection and clean up power supplies in addition to providing backup power.

9.2. Power over Ethernet

Some devices, such as cameras, make extensive use of Power over Ethernet. While convenient, this is not necessarily a plug and play. Care must be taken to ensure that the power sourcing equipment (PSE) is sufficient for all powered devices (PD) connected to it, especially taking the cabling into account. There will always be some power loss over the cable, and with higher gauge wires and longer lengths, sometimes this can be significant when there are a number of PDs. Be sure to take into account the devices worst case power (e.g. startup) not just its typical power. An example is when power is reapplied to all devices at the same time after a power outage. The devices power draw could briefly be quite high which could temporarily exceed the current capacity of the PSE, if it is not sufficient.

Also take into account that when a PD's device's cable is removed, it can cause arcing which can lead to pitting of the connectors. Therefore, it is recommended that the connector be examined during any maintenance to ensure that there is no pitting (also check for corrosion).

As always, be sure to have protection for voltage surges caused by lightning.

9.3. Batteries

9.3.1. Battery Overview

Lithium batteries, if not handled correctly, can be very dangerous. Every service provider *should* supply training on proper lithium battery handling. It is outside the scope of this document to define this material; however, the OSHA and UL sites have material on this.

In general, batteries have several issues for service providers:

1. Limited life (even rechargeable batteries), therefore the need to be replaced periodically
2. Limited environment
3. Low power limits sensor capabilities
4. Recycling

For more information on batteries, the following report is recommended:
https://www.nctatechnicalpapers.com/Paper/2019/2019-methods-to-maximize-iot-battery-life

9.3.2. Battery Lifetime

9.3.2.1. Non-Rechargeable Batteries

Non-rechargeable batteries will need to be replaced periodically. Therefore, it is important for a service provider to take this into account in their pricing strategy and planning. While many people can replace the batteries, if the service provider offers a replacement service, most customers will utilize that method. Therefore, the service provider needs to have a strategic plan on how to approach battery replacement.

The service provider needs to determine for each type of device whether they will do a proactive maintenance replacement of the batteries before they fail or a reactive replacement after they fail. This is a case where remote monitoring provides a key indicator (battery status) that can be used for proactive replacement. This saves money in that battery replacements and servicing only happen on an as needed status. Otherwise, a periodic replacement plan can be implemented or the service provider can be reactive by replacing the battery when the customer calls to report a low battery or non-responsive (dead battery).

One way to minimize truck rolls for battery replacement is to implement a process where if a service technician is at a particular site, a check is done to determine if any of the battery-powered IoT devices is reporting that it has week or low battery that needs replacement, or that it is within a window for replacement. The technician can then replace the battery to prevent a truck roll in the future.

9.3.2.2. Rechargeable Batteries

Many of the rechargeable batteries require a battery management circuit. One of the values that can typically be supplied from these is the battery health. When the battery health has reached a certain point, for example for battery backup where it cannot provide power for the desired time, then remote monitoring *should* provide a notification that the battery needs to be replaced. If a remote monitoring system is not implemented, then methods similar to the non-rechargeable batteries *should* be implemented for replacing the batteries. However, in the long run, a remote monitoring system will greatly decrease battery waste and save money for the service provider.

9.3.3. Limited Environment

The typical operating temperature for an inexpensive battery is within a narrow margin, primarily meant to operate within a controlled indoor environment. Any battery-operated devices which are intended to operate outside need to ensure that the battery is rated for the outside temperatures within that geographic region, especially if the device is exposed to the sun or is within an enclosed area. Note that thermal statistics are extremely important for the replacement batteries as well. Be sure that processes are set up to ensure that the correct battery type is replaced.

Additionally, altitude needs to be considered. Some batteries have outgassing protection which can cause issues at higher altitude.

While vibration is generally not a problem once deployed, it can be a problem during shipping. Also, the batteries do need to be able to survive common drops (e.g. 1 meter onto a concrete floor, both by itself and within the IoT device).

9.3.4. Battery Operated Sensor Capabilities

In general, wireless sensors which are battery operated tend to be transmit-only devices that transmit when an event occurs or at a periodic interval. As an example, a door sensor only needs to transmit when the door is opened, when it is closed, and when the battery level is low. Different technologies are used which minimize the transmit time, and many of them guarantee message delivery.

One important item to be aware of is that technologies which share unlicensed spectrum (e.g. ISM bands), can utilize multiple transmissions when there is a signal collision and cause the battery to deplete faster than expected. A good example is ZigBee whose channels share the spectrum with the Wi-Fi 2.4 GHz channels. While this is dependent on the country, it is recommended that ZigBee be set to a channel either outside or on the edge of the Wi-Fi channels. Then, if possible, the local Wi-Fi *should* be set on a channel away from the selected ZigBee channel.

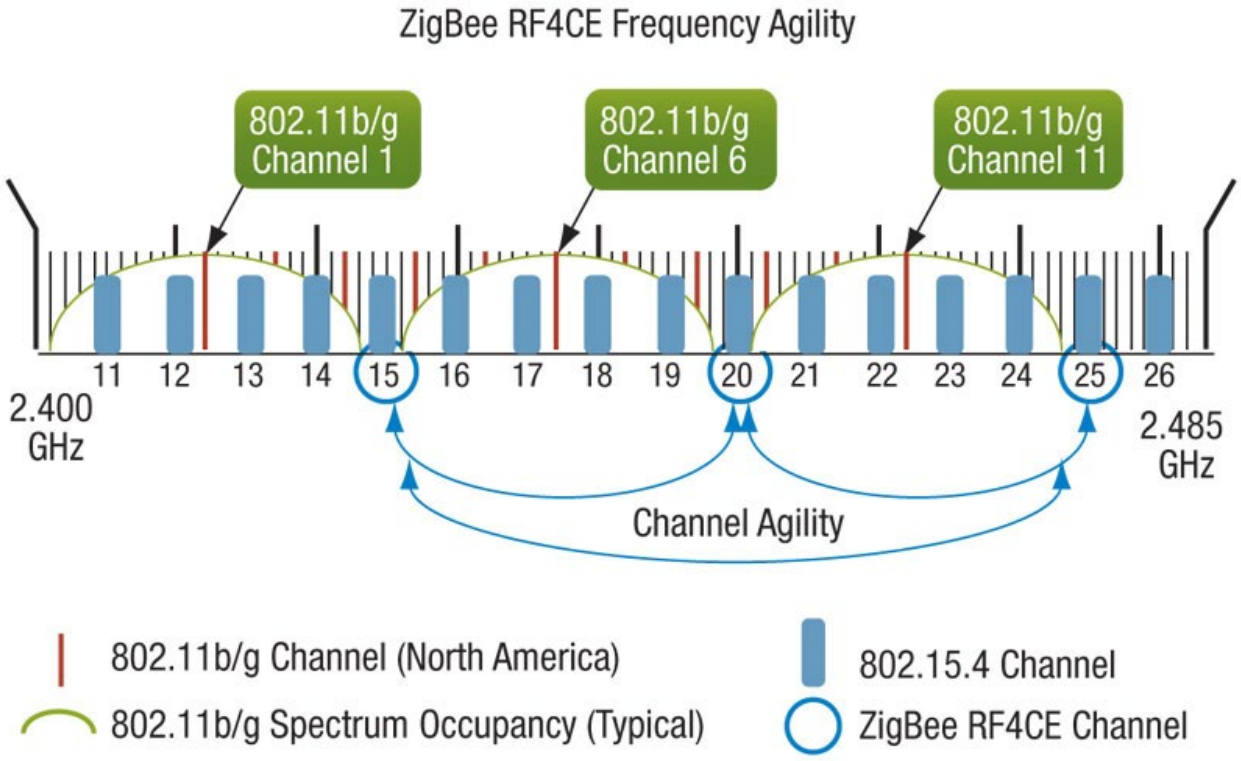

Figure 2 - ZigBee and Wi-Fi Channels

9.3.5. Recycling

Many of the service providers are recycling lithium batteries. Not only is this a good environmental practice, but it can also be economical. Be sure to follow all the handling guidelines even with depleted batteries as they can still be dangerous if mishandled.

9.4. Power over Coax

While not used very often for IoT purposes, power over coax has been utilized for a long time to power in-home amplifiers. The primary concern to be aware of is that if DC voltage is utilized that there cannot be dissimilar metals, especially in connectors, which would cause galvanic action, which would lead to failure of connectors over a period of time.

10. Other Considerations

10.1. Connectors

Connectors are required but can be the bane of problems. It is important that the correct high-quality connector be utilized. Having to continuously make a trouble calls to correct a poor quality connector is not good practice. Well designed, standards-based connectors can help minimize unexpected failures and ultimately unsatisfied customer experiences.

Generally, a good connector in an indoor setting will give minimal problems. However, outdoors can be a problem even with the best connector. The biggest problem is keeping moisture out of the connector, which can cause corrosion to the connector housing, the wires connecting to the connector, and the contact areas. Also, be aware that water can wick up through the wires and damage them far from the connector itself. Whichever method is used to seal the connector, be sure that it is capable of operating in the expected temperature range and that it is not affected by the ultraviolet light from the sun.

10.2. Severe Environmental Areas

Even though it seems obvious, do not install inside IoT devices outside, even if they seem to be in a protected area. Aside from the extreme temperature ranges, there is always the problem of moisture.

If an IoT device is intended for outdoor use, be sure to follow the vendors directions and guidance. If there are any questions, contact the vendor. They are usually very cooperative to service providers.

For the cases where an IoT device is in an indoor area with a severe environment, mainly for businesses, use care to ensure that the device is fully operational under the worse circumstances. Again, follow the vendor's directions and guidance. Also understand that sometime there might not be a device in your inventory that will work for all possible customers. Sometimes you just have to say no, but when you do, be sure have a local business that would offer what the customer needs.

10.3. Pests

Pests can be a major problem if they can get into the IoT device. Roaches are some of the worst, as they are attracted to vent holes, and once inside they have trouble getting out. Dead roaches then release a smell which attracts other roaches, and the device soon fills up with roaches. Therefore, it is best if the device does not have any ventilation holes, although sometimes this is impossible. If there is ventilation holes, then the devices *should* have a grid to prevent roaches (and other pests) from getting inside.

Other problems occur when pests (or pets) like to gnaw on the wires. This is very difficult to prevent other than trying to keep the wires as short as possible.

11. Customer Education

When working directly with the customer, it is recommended to try to explain to them what the IoT devices are for, not to move them, not to spray anything into them, or do other activities that can cause

damage or faults. If a device has batteries, then a process needs to be developed by the service provider to inform the customer when the batteries need to be replaced, and then either have a step by step method to walk the customer through replacing the batteries or plan for a truck roll to replace the batteries. If lithium batteries are used, then there *should* be a mechanism to collect and recycle them, All collected batteries *should* be properly disposed of and recycled where possible.